# EVIDENTIARY CONSIDERATIONS FOR EPA'S USE OF ELECTRONIC REPORTING

## I. INTRODUCTION

This paper discusses evidentiary issues that may arise whenever an environmental agency, such as EPA, seeks to introduce electronic reports and/or data in an enforcement case. This analysis assumes that EPA will most likely use electronic reports in two types of actions: (1) criminal enforcement cases, including actions for fraudulent filing or falsification of reports, and (2) civil or administrative enforcement cases for violations of environmental statutes. Because the evidentiary rules are essentially the same for civil and administrative enforcement cases, they are included together here as "civil" cases.

In both criminal and civil enforcement cases for violations of environmental statutes, EPA may need to use an electronic report, and the information contained within it, to prove any or all of the following:

- That the report was sent (or not sent);
- When the report was sent;
- By whom the report was sent, whether a corporate entity or an individual signer of the report; and
- What the report contained, so the data can be compared to other evidence of pollution or to standards set by regulation or permit for air emissions, water discharges, or volumes of hazardous waste disposed or transported.

EPA will also need to prove that the report was received by the agency and was electronically stored and retrieved without any changes.

In criminal fraud cases alleging falsification of electronic reports, proof of the same information described above will have to be offered by EPA. In addition, proof must be offered regarding the falsity of the reports and the defendant's intent and knowledge with respect to the

fraudulent filing of the report. An accompanying memorandum outlines the variety of EPA criminal actions which might involve electronic reports.

The major distinction in successfully prosecuting a civil case and a criminal case is the relevant burden of proof. Civil cases must demonstrate violations by a preponderance of the evidence, whereas a criminal case must be proven beyond a reasonable doubt. However, the kinds of evidence or means of proof are essentially the same in both criminal and civil cases. The major difference is how much evidence or testimony on each issue is needed to meet the burden of proof. In a civil case, the evidence and testimony must be enough to persuade a reasonable juror that the government's position is more likely correct than not. But in a criminal case, the evidence must be sufficient to eliminate any reasonable doubts in the jurors' minds about the correctness of the government's position and the guilt of the defendant.

With these practical applications in mind, this paper reviews the existing evidentiary rules under federal law based on the Federal Rules of Evidence (FRE), which apply equally to civil and criminal actions. Different evidentiary rules may apply, however, in state enforcement cases. Evidentiary rules govern how documentary evidence, including electronic reports, can be introduced in all types of enforcement cases, both criminal actions for fraudulent filing of reports as well as criminal and civil actions for violations of environmental statutes. There are still some unanswered questions about whether electronic data is documentary evidence because it exists in electronic format only. This paper assumes, however, that EPA will still present electronically transmitted reports to a judge or jury in a paper format.

This paper also assumes that there are no special federal court rules, statutory provisions or agency regulations related to the use of electronic data as evidence. As far as can be determined, it appears that no such special rules, statutory provisions or regulations would apply to EPA's use of electronic data as evidence in civil or criminal cases filed in federal court. Some states, however, have already adopted special statutes and agency or court rules governing the use of electronic data; but these provisions have not been analyzed or considered in this paper.

Section II of this paper focuses on the evidentiary rules that will apply to introducing traditional paper documents as evidence. This situation is the closest analogy for determining what rules might apply to electronic reports. There is some relevant case law at the federal level and also some case law in state courts related to the introduction of electronic data as evidence, but these state court decisions may or may not be persuasive to a federal court. Taken together, however, these decisions are contradictory. Because this issue is so new, there is not yet any clear federal rule of law governing the introduction of electronic reports as evidence. The

discussion in Section II is therefore limited to the FRE and the types of proof that might be needed in order to admit electronic reports under those rules.

In Section III, this paper outlines the kinds of evidence -- both witnesses and documents, whether electronic or paper -- that EPA will need to prosecute successfully a criminal fraud case related to electronic reports. It builds on the rules of evidence as outlined in Section II, which all apply to the use of electronic reports in a criminal fraud action. Section III highlights the additional types of evidence and information about the reports that EPA may be required to introduce in order prove an electronic report is fraudulent or has been falsified. Some of these items of proof may not be necessary, however, for EPA to prevail in civil or criminal enforcement actions for violations of environmental statutes.

Section IV uses two scenarios to illustrate how the evidentiary rules and legal requirements for criminal fraud and civil enforcement cases would actually be applied. It explains the types of proof and testimony needed to bring two types of legal proceedings: (1) a criminal action for falsification of data in discharge monitoring (DMR) reports, and (2) a civil enforcement action for violations of emission limits in an air permit which relies upon continuous emissions monitoring reports (CEMs) to prove the violations. Section IV does not, however, take into account the technological or other solutions which may be available to address these evidentiary issues.

Based on the principles of evidence for using electronic reports in enforcement cases (Section II) and the nature of the additional proof required for criminal fraud actions (Section III), Section V of this paper briefly identifies the areas of proof that are critical to successful EPA prosecutions using electronic reports and are relevant to developing and implementing EPA's policy on electronic reporting.

## II. RULES OF EVIDENCE APPLICABLE TO ELECTRONIC REPORTS IN ENVIRONMENTAL ENFORCEMENT ACTIONS

In future enforcement cases, EPA will need to introduce into evidence printed versions of a series of electronic reports from a regulated entity. The fact-finder will be asked to accept the content of the printed reports as being the same reports that were submitted to EPA by the regulated entity or individual charged in the case. Depending on the nature of the case and the jurisdiction in which it is filed, the fact-finder could be a judge, a jury, or an administrative law judge. For simplicity, we refer to them collectively as "the fact-finder."

EPA will be asking the fact-finder to conclude that the reports were filed by a certain person on a certain date. In an action to prosecute an individual for filing a fraudulent report, EPA will also be seeking to admit the reports into evidence to prove that the data they contain, such as discharge monitoring data, are false and do not accurately reflect the chemical parameters of the permittee's discharges, emissions or wastes at the time of monitoring.

Federal courts, through the FRE, have established multiple rules to ensure that "documents" admitted into evidence for the truth of the statements contained therein are authentic and reliable. First, a witness or witnesses who are knowledgeable about a document, its creation, receipt and/or storage, must testify to establish the foundation for admitting the document into evidence. Depending on the extent of foundation testimony required, more than one witness is often needed before a fact-finder will allow documentary evidence to be admitted.

Second, a witness or witnesses must give testimony to prove that a document is relevant and competent. Relevance is established by proving that the document is the "best evidence" available and does not contain hearsay. Hearsay could be any statement or data in the document for which the truth cannot be tested through cross-examination of the person who allegedly made the statement or entered the data. Some aspects of the competence of the document can be established in an EPA action for fraudulent reporting by testimony of witnesses who can authenticate the creation, receipt, storage or retrieval of a report.

In jury trials, a judge will determine whether documentary evidence is admissible by deciding whether it is relevant and competent before it is ever viewed by the jury. It is possible, however, that once a report is deemed admissible by a judge, the jury may nevertheless disregard such documentary evidence or give it less weight than necessary to sustain the government's

burden of proof if the jury doubts the genuineness or credibility of the evidence. Sections II.A and II.B below discuss in more detail the requirements for demonstrating that documentary evidence is both relevant and competent.

A. Relevant Evidence

FRE 401 requires that evidence must be material and probative before it can be admitted into evidence for consideration by the fact-finder. This requirement means that each item of evidence must tend to prove or disprove a material fact or issue. The contents of electronic reports clearly are such material facts. In a criminal fraud case, the content of the electronic report is itself the fraudulent statement. In other criminal or civil enforcement actions where violations of environmental standards are alleged, the contents of the electronic report likewise become material evidence and will be a central element of the government's case.

The rules about whether documentary evidence is probative or relevant focus on the content or substance of the documents offered into evidence and are designed to ensure the reliability of this evidence.

1. Best Evidence Rule

The best evidence rule, commonly referred to as the “original document rule,” requires that the "original" of a document be submitted into evidence to increase the credibility of the document's contents and to reduce the risk of tampering or inadvertent change to its contents through reproduction. In order to accommodate the realities of modern-day business, however, an exact duplicate (such as a xerox copy) is admissible as an original unless the authenticity of the original is challenged or if it would be unfair, under the circumstances of the case, to admit the duplicate. FRE 1001(4) and 1003. FRE 1001(3) specifically addresses the best evidence rule with respect to electronically stored data by providing that any printout or other output "readable by sight" and shown through witness testimony to reflect accurately the data stored in the computer is considered an "original."

Courts have often not relied on the best evidence rule, however, to determine whether electronic data is admissible in a given case. Rather, they frequently require a number of witnesses to provide extensive authentication testimony and then conduct a detailed analysis of whether the electronic data and associated reports qualify under the business records and other applicable exceptions to the hearsay rule.

2. Hearsay

FRE 801(c) defines hearsay as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." A computer printout reflecting electronic data, offered into evidence to prove the truth of its contents, is hearsay. Courts traditionally have found hearsay evidence to be inadmissible unless it falls under one of the exceptions to the hearsay rule. Hearsay evidence is considered by courts to be inherently unreliable under the assumption there is no witness available for cross-examination so the opposing party cannot explore the truth or falsity of the statements made in a hearsay document or by a hearsay witness. Exceptions to the hearsay rule that are relevant to electronic reports are described below.

a. Admissions

In cases where the opposing party created the document sought to be admitted into evidence, the most direct way to avoid the prohibition of the hearsay rule is to assert that the evidence is an admission by a party opponent and thus not hearsay at all. FRE 801(d)(2)(C) provides that such an admission is "a statement by a person authorized by the party to make a statement concerning the subject." FRE 801(d)(2)(D) provides that an agent's statement can be an admission against the agent's employer. Statements made by the opposing party are often considered by the courts as "admissions against interest" and are viewed as inherently reliable. A court will determine, as a matter of law, whether this admission exclusion to the hearsay rule applies to a particular document, and witness testimony on this legal point may not be necessary.

When paper reports filed by regulated entities are sought to be introduced as evidence, EPA can seek to establish the reliability of the information contained in those reports by arguing that they constitute an admission by the regulated entity, are not hearsay, and are inherently reliable. This argument has been acceptable to the courts under the FRE because changes to a written document are usually readily identified. It is not possible to predict yet whether courts will conclude that electronic reports are, in and of themselves, reliable evidence and can be treated as admissions by their submitters. It is possible that, for some judges and juries, the unknowns in the technology of electronic reporting will raise questions about the reliability of these reports and thus prevent them from being accepted into evidence as inherently reliable admissions against interest.

b. Business Records

The "business records" exception to the hearsay rule has been analyzed by several courts to determine whether electronic reports constitute inadmissible hearsay. Under FRE 803(6), electronic records that satisfy the following requirements, proven through witness testimony, will be admitted into evidence under the business records exception to the hearsay rule:

- The document must have been created by a "business";
- The document was created in the regular course of business;
- The person who created the document must have had personal knowledge about the information reflected in the document;
- The document must have been created at or near the time of the event recorded; and
- The document must be authenticated, usually by the business' own custodian of records (see discussion of document authentication in Section II.B.1 below).

Courts asked to review electronic reports as business records usually hear extensive testimony regarding the hardware and software involved in entering, storing, and retrieving the data at issue. Proof regarding the regularity of the computer process generally satisfies courts, in the context of commercial transactions, that the a computer-generated document is sufficiently reliable to be admitted into evidence under the business record exception to the hearsay rule.

There is case law to suggest that a statutory obligation to keep records -- such as the requirement to submit DMRs, CEM reports or hazardous waste manifests -- is a duty created in the "regular course of business." While EPA may rely on this fact to prove the second component of the business records exception, witness testimony may still be required to prove the other components, including that the person who created the electronic report had personal knowledge of its contents, that the report was recorded near the time of the event, and that the document is "competent" evidence as explained in the next section.

### B. Competent Evidence

Once it has been established that documentary evidence is relevant and does not violate an exclusionary rule -- it has been proven to be an "original" and it does not contain inadmissible

hearsay -- proof must be presented on two elements regarding the competence of the evidence. First, witness testimony must be offered to "authenticate" the document by showing how it was created and how it was maintained after its creation in order to demonstrate that the contents of the document are genuine. Second, testimony must be provided to prove the "chain of custody" and to show that the document has not been altered since it was created.

The courts determine competence of evidence by examining how a document was created and where it has been at all times until the moment it is presented as evidence in court -- the procedural history of the document, as opposed to its contents. The courts have also created some evidentiary presumptions to simplify this proof for documents created or maintained in certain circumstances, as discussed in Section II.B.2 below.

1. Authentication

Authentication of a document is proof that the writing is what the proponent claims it to be. This evidence often includes proof that the writing was made or signed by a particular person, or that it has been adopted by that person's subsequent actions. Proof for authenticating a document must be sufficient to convince the judge that the document is genuine. Once the judge has decided to allow a document to be admitted into evidence, the judge or jury will later determine whether the document is credible or persuasive on the matters for which it is offered as proof.

Some documents are self-authenticating, based on the circumstances surrounding their execution. For example, certified copies of public records and documents accompanied by a certificate of acknowledgement, such as the seal of a notary public, can be admitted into evidence without authentication testimony. Most documents, however, must be authenticated through witness testimony before they can be admitted into evidence and then considered later as to their credibility or persuasiveness.

a. Admissions

The most direct way to authenticate a document is through an admission by the party opponent that the document is genuine. An admission to authenticate a document can be obtained through the discovery process or by stipulation of the parties, which is separate from an admission created by the FRE and used to overcome any hearsay objections to a document.

The discovery process is a means for each party to learn relevant information about the

details of a case from each other and from others not party to the case. In civil actions, the discovery process can include depositions (oral questions to be answered under oath), interrogatories (written questions to be answered under oath), and requests for admissions (to be answered under oath). In criminal actions, the discovery options are more limited. They include search warrants, grand jury subpoenas and trial subpoenas and, under the provisions of FRE 16 for reciprocal discovery, a criminal prosecutor must divulge any exculpatory evidence to the defendant. Because criminal cases have these limited discovery options and the higher burden of proof beyond a reasonable doubt, authentication of a document by admission is less likely in a criminal action.

b. External Proof of Authenticity

In cases where no admission of genuineness can be obtained, witness testimony must be introduced to authenticate a document. This proof can include any type of evidence, including circumstantial evidence which tends to establish the genuineness of the document. Testimony can be offered of witnesses who saw the document being created or signed or who heard it being acknowledged by the author or signer. Documents are often authenticated through handwriting analysis, in which testimony of an expert is offered to verify a person's signature. Proof can also be offered regarding the subsequent actions of the document's author in reliance on the document.

Authentication of electronic reports may be problematic for several reasons. First, the evidence does not exist in readable format without additional data manipulation, which automatically raises questions about authenticity. Second, electronic reports do not have a commonly recognized "signature." Third, there is no consistent case law defining what constitutes a reliable "signature" for electronic reports. For the electronic reports, the government is not likely to have easy access to circumstantial evidence -- such as witnesses who saw the report being entered into the computer or the defendant’s own later actions in reliance on the report -- which would usually be available in cases based on paper to prove that the contents of a document are genuine.

c. Technological Processes

There are special rules for authenticating documents created by a technological process -- such as x-rays, EKGs, and ballistics tests -- as distinguished from paper documents created by a person. FRE 901(b)(9) provides that such documents can be authenticated by presenting evidence describing the technological process or system and by showing that the process or

system produces accurate results. Proof of each of the following elements is required:

- o The technological process is accurate;
- o The machine (the "hardware") was in working order; and
- o The operator was qualified to operate the machine.

Courts often take judicial notice that a certain technology is accurate, eliminating the need in future cases to provide testimony on this point. Most courts take such judicial notice in the case of x-rays, EKGs, radar, ballistics and blood tests. However, such judicial notice has not generally been taken for the process of electronic data creation, transmission, storage and retrieval.

It also very important to remember that judicial notice of a technological process will not be determinative in a criminal action because the jury is allowed to reach its own conclusions regarding the validity and reliability of a technological process. FRE 201(g). In criminal cases, the prosecutor usually produces several witnesses who offer extensive testimony about the technological process itself in order to make the process understandable and credible to the jury.

The electronic reports that EPA may introduce in enforcement and fraud cases would be a combination of documentary evidence created by a person (the printed version of the report itself) and technological evidence (the process used for creation, transmission and storage of the electronic report). The witnesses who testify to authenticate an electronic report must therefore be able to address both aspects of the document: (a) the submitter's creation or preparation of the report and the accuracy of the data contained in the report as a reflection of the submitter's activities, and (b) the computer processes used by both the submitter and by EPA to transmit, store and retrieve that data. In cases involving allegedly false reports, testimony of witnesses with first-hand knowledge of these two areas would be needed to demonstrate the genuineness of the reports which EPA retrieves from its computer and offers as evidence in court. Likely witnesses would thus include employees of EPA and the regulated entity.

2. Evidentiary Presumptions to Prove Chain of Custody

Regardless what type of authentication testimony is offered, chain of custody must also be proven to show that a document has not been altered since it was created. For tangible evidence, such as a water sample, an unbroken chain of custody is proven by testimony

documenting that each time physical possession of the sample changed hands, someone double-checked to be sure the sample had not been tampered with. In the case of electronic reports, it is possible that proof of an unbroken chain of custody will require testimony regarding each time the data moved in and out of a file, with verification that no changes to the data were made, or were possible, in each instance.

Several evidentiary presumptions have been created by the courts to make it simpler to prove the chain of custody in certain factual situations. There is a presumption of regularity regarding certain government actions. Thus, absent case-specific proof to the contrary, courts generally assume that the government acts reliably in maintaining records and data it receives from private parties. It is unknown whether courts will apply this presumption of regularity to electronic reports received and stored by the government.

There is also a presumption of mail delivery and, absent case-specific proof to the contrary, courts assume that a letter which was properly addressed, stamped and mailed has been delivered. As yet, neither court decisions nor the FRE provide any analogous presumption for delivery of electronic reports.

In cases where the party offering a document as evidence can rely on an evidentiary presumption to avoid having to prove the chain of custody, consideration should also be given to whether the fact-finder will have sufficient confidence in the chain of custody to find the document reliable without further proof. Thus, in the case of electronic reports, a jury having minimal personal experience with computers might need to hear evidence about the submitter's computer process for entering the data, creating the report and sending it, as well as the agency's process for receiving, storing and retrieving the data. Otherwise, the jury may not be convinced beyond a reasonable doubt that the report being introduced into evidence is, in fact, the same report that the regulated entity prepared and transmitted; and the presumption of the regularity of government activities may not be sufficient to overcome their doubts.

Because this area of the law is so new, there is currently no certainty regarding the evidentiary rules that a court will apply to the admission of electronic reports. However, a decision of the Sixth Circuit[1] highlights the various components of the foundation testimony that will probably be required to convince a court to admit electronic reports into evidence:

---

[1] *U.S. v. Russo*, 480 F.2d 1228 (6th Cir. 1973).

> ... [T]he foundation for admission of [computerized records] consists of showing the input procedures used [and] the tests for accuracy and reliability... . The [opposing] party then has the opportunity to cross-examine concerning practices with respect to the input and as to the accuracy of the computer as a memory bank and retriever of information. ... [T]he burden of presenting an adequate foundation for receiving the evidence should be on the party seeking to introduce it rather than upon the party opposing its introduction.

Based on the Russo court's analysis, it is likely that, in an environmental case alleging fraud or false reporting, a proper foundation for admission of electronic reports will require witnesses who can testify to all of the following steps in the data transfer process:

- Data creation,
- Entry of data into the computer,
- Transmission of data from the creator to recipient,
- Storage of the transmitted data by the recipient, and
- Conversion of the electronic data into a paper document to be viewed by the fact-finder.

Thus, in cases involving electronic reports submitted to EPA, prosecutors will need testimony from the individual employees of the regulated entity who created, entered and transferred the data, as well as from the EPA staff who received, stored and retrieved the data to prepare the written document presented to the fact-finder.

## III. CRIMINAL FRAUD

Criminal fraud is an enforcement option for EPA in cases where a regulated entity, or one of its employees, has made false statements in electronic reports. Criminal fraud can be brought under various substantive environmental statutes[2] or under 18 U.S.C. §1001, the False Statements Act (see accompanying memorandum on criminal actions). Criminal fraud cases can be filed against the regulated entity making the false statement (a corporation or partnership) or against the individual employed by that entity who is responsible for submitting the false statement to the government -- usually the person who signed the false report -- or against both.

For most criminal fraud cases, the following elements must be proven to obtain a conviction:

- The defendant made a statement;
- The statement was false;
- The defendant knew the statement was false, fictitious or fraudulent when made;
- The defendant made the false statement with the intent to deceive;
- The false statement was material; and
- The false statement was made in a matter within the jurisdiction of the department or agency of the federal government prosecuting the case.

Electronic reports are essential evidence in criminal cases for fraud or false statements, just as they can be crucial in other enforcement actions for violations of environmental statutes. In criminal fraud cases, some aspect of the report and the data it contains <u>are themselves</u> the false statement. Electronic reports must therefore be introduced into evidence as part of the

---

[2] See, e.g., Clean Water Act, 33 U.S.C. §1319(c)(4); Clean Air Act, 42 U.S.C. §7413(c)(2); Toxic Substances Control Act, 15 U.S.C. §2614; Resource Conservation and Recovery Act, 42 U.S.C. §6928(d)(3); Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. §9603(b).

prosecution's case in chief.

As described in Section II above, the evidentiary rules for proving the relevance and competence of documentary evidence will apply equally in a criminal fraud case. The primary difference is the government's higher burden of proof in the criminal fraud case. The prosecution must persuade the jury beyond a reasonable doubt that the paper version of the electronic reports submitted into evidence by the government contain the identical information and data as the electronic reports prepared and submitted by the individual or corporate defendant accused of criminal fraud.

In a criminal fraud case, another critical element of proof relating to the reports themselves is the identity of the person who submitted the false reports to the government. This proof must tie the false reports to the individual defendant. In cases involving paper reports, identity is proven by the defendant's signature. Because proof of the defendant's identity in a criminal fraud case must be beyond a reasonable doubt, the level of certainty regarding the identity of the signer and his/her signature must be quite high.

If the defense counsel in a criminal fraud case can create any "reasonable doubts" about the reliability of the evidence that the defendant is the person who signed the reports, the government may not be able to obtain a conviction. Such reasonable doubts can even be raised by cross-examination alone. In the case of electronic reports, therefore, a criminal defendant is likely to challenge the security and reliability of the both electronic signature process and the processes for data transfer, storage and retrieval in order to create such a reasonable doubt. It will be the government's burden, as the prosecutor, to prove beyond a reasonable doubt that a particular individual -- in some cases, a person working for a corporate defendant -- is the person who electronically filed the allegedly fraudulent reports.

The electronic data creation, transfer and storage process will also be an important element of the government's evidence to prove an individual defendant's intent and knowledge in filing the reports and making false statements. The government's proof must demonstrate the defendant's knowing and willful falsification, as well as demonstrating an intent to deceive. Testimony about the level of security incorporated into all steps of the electronic data transfer process may help EPA to persuade the jury that the defendant had knowledge of the deception and intended to deceive the government. In other words, if the government can show that the defendant must have had detailed knowledge and understanding of the regulated entity's entire system for preparing electronic reports, submitting them and signing them and was thus able to alter the data before transmitting it to EPA, a jury might reasonably conclude that such actions

were knowing, willful and intentional.

## IV. TWO EXAMPLES OF CASES INVOLVING ELECTRONIC REPORTS

This section applies the evidentiary rules discussed in the Sections II and III to two hypothetical scenarios typical of the cases EPA might bring based on electronic reports. This detailed description of the witnesses and testimony that would be presented to a fact-finder in each case is intended to illustrate more clearly the practical impacts of the evidentiary rules in both criminal fraud and other enforcement cases involving electronic reports.

### A. False DMR Scenario

Company A submits a series of electronic water discharge monitoring reports (DMRs) to EPA which, on their face, reflect compliance with most of the discharge limits in the company's permit. EPA later learns that some of the data in the DMR reports are false and do not accurately reflect water discharges at Company A's facility. In fact, Company A has falsified its DMRs. EPA decides to file two actions for criminal fraud: one against Company A, and one against Individual S, the Company A employee who electronically "signed" the DMR reports.

To sustain its burden of proof in a criminal fraud action, EPA will need to prove all of the following elements with respect to <u>each</u> electronically filed DMR to be entered into evidence:

- The electronic DMR was sent to EPA;
- By Company A;
- The DMR was electronically "signed" by Individual S;
- Individual S was authorized by Company A to sign and submit the DMR;
- The DMR was received by EPA;
- The data contained in the DMR, as received by EPA and submitted in printed form to the fact-finder, are identical to the data electronically submitted by Company A;

- o Some of the data contained in the DMR are false;
- o Individual S knew the data were false when he/she signed the DMR reports; and
- o Individual S intended to deceive EPA by submitting the false data in the DMR reports.

Two other elements of a criminal fraud action are not discussed here. EPA will have to prove that the falsified DMR data are material in this case, which can be done by showing that other real water monitoring data demonstrates the falsity of the data in the electronic DMRs. EPA will also have to show that the false statements -- the DMR data -- were made in a matter within EPA's jurisdiction.

EPA will rely on the DMR reports themselves to prove that both defendants (Company A and Individual S) submitted the electronic DMR reports and that Individual S electronically "signed" the DMR reports, which were then electronically submitted to EPA by Company A. EPA will, therefore, need to have the DMR reports introduced into evidence and have the fact-finder accept the data in the electronic DMRs as relevant and competent. To have the DMRs introduced into evidence, EPA will therefore need to provide witnesses who can testify about the relevance and competence of the DMRs.

EPA must prove that the written DMR reports submitted into evidence, which have been printed by EPA on the basis of the data EPA retrieves from its computer, are the best evidence available and do not contain inadmissible hearsay, thus satisfying the requirements of the business record exception to the hearsay rule. The DMR reports and the data contained therein must also be authenticated, and an unbroken chain of custody must be proven from the time individual S at Company A entered the data into its computer to create each of the reports and electronically signed the reports to the time the prosecutors introduce the DMRs into evidence at trial.

Absent any specific evidentiary rules or presumptions applicable solely to electronic reports, EPA will need to follow a process something like the following to be able to introduce each relevant DMR into evidence:

1. Establish that the DMR is authentic, that it was in fact sent by Company A:

   a) By stipulation or agreement from Company A (which is unlikely in a criminal

case);

b) If no stipulation, by specific evidence tending to prove authenticity, such as:

i) An identifying electronic signature;

ii) A provision of the TC&A which authorizes introducing the DMR into evidence;

iii) By direct evidence from witnesses about the preparation and transmission of the DMR; or

iv) By circumstantial evidence proving where and how the DMR was created.

2. Establish that each DMR is relevant by proving that the information originally entered by Individual S, as an employee of Company A, in creating the report at the beginning of the process has remained unaltered and that the information and format of the printed version of the report offered by EPA are therefore appropriate for introduction into evidence:

a) By stipulation (not likely in a criminal case);

b) If no stipulation, by specific evidence tending to prove relevance, such as:

i) A provision of the TC&A which authorizes introducing the DMR into evidence; or

ii) By evidence about the methods and processes for data entry, submission, transmission, downloading, storage, retrieval and conversion to a paper format usable for litigation purposes.

3. Establish that introduction of each DMR is not otherwise objectionable, such as due to potential hearsay issues:

a) By stipulation (again not likely in a criminal case);

b) Because the information contained in the DMR is an admission by Company A; or

c) Because the information contained in the DMR qualifies under the business records exception.

Witnesses who are employees of both Company A and EPA must testify in cases where EPA needs to submit evidence about:

- The preparation and transmission of the DMRs;
- The methods of entering, transmitting, downloading, storing and retrieving the DMRs; or
- To lay the foundation for the business records exception to the hearsay rule.

These witnesses must be individuals who are familiar with the computer hardware and software involved in electronic data entry, submission, transfer, storage and retrieval. As a named defendant, Individual S is not likely to be cooperative unless he or she pleads guilty and agrees to testify against other Company A officials who may have ordered the filing of false DMRs. It unpredictable whether other Company A witnesses will be cooperative or hostile but, because Company A may be at risk for criminal penalties, these witnesses are also not likely to be cooperative.

In general, however, Company A witnesses would be called by EPA to provide details about the procedures used to gather the data, to create the electronic report by entering the data into the computer, and to submit it electronically to EPA. Testimony would also be requested from Company A witnesses regarding the “electronic signature” or other means of electronically "binding" the DMRs to individual S as the employee of Company A who prepared the reports. EPA witnesses will then need to supply testimony to document the remaining chain of custody upon receipt of the data by EPA’s computer. The EPA witnesses' testimony would provide details regarding EPA’s process for receipt, storage, retrieval of Company A’s data, and transfer of the data into the written report submitted as evidence at trial.

After hearing the testimony of Company A and EPA witnesses, the fact-finder will then compare (1) the reports and data contained therein that were electronically transferred by Company A to (2) the printed DMRs offered as evidence by EPA to determine if those documents are relevant and competent. If it concludes that they are, the relevant DMRs will be accepted into evidence.

In laying the appropriate foundation for introducing false electronic DMRs into evidence, criminal fraud cases will differ from other enforcement cases involving electronic reports in four critical respects.

First, it is unlikely that the defendants in a criminal fraud case will stipulate that the DMRs are authentic and have remained unchanged since their creation. Witness testimony will likely be necessary in a criminal case to prove that DMRs are authentic, relevant and not subject to a hearsay exclusion. Witnesses for this aspect of the case will include Company A employees, who will need to testify about the data creation, input and transfer procedures at Company A's end. After this testimony, EPA staff familiar with the computer processes will have to testify about EPA's end of the data transfer, storage and retrieval process. The proof must be adequate to persuade a jury beyond a reasonable doubt that the written DMR reports presented by EPA as evidence are identical to the data electronically submitted by Company A and Individual S.

Second, in order to convict both Company A and Individual S, the testimony offered by EPA in the criminal fraud case will have to prove beyond a reasonable doubt that Individual S was the person who electronically "signed" and submitted the DMRs. If EPA cannot provide this proof, it is very unlikely that Individual S can be convicted for criminal fraud.

Third, EPA must demonstrate that data in the DMR reports were false. Proof for this element of the criminal fraud case will come from witnesses and evidence that are unrelated to the electronic reports. Proof that Company A's actual water discharges were different from the data in the electronic DMRs will probably be found in EPA's own sample results or the company's actual sample results or original lab reports. EPA would discover such evidence through criminal investigation techniques or obtain the company's actual results from an honest employee of Company A, an employee who was recently fired or had become otherwise disgruntled, or perhaps whistleblower.

Fourth, EPA will need to submit proof regarding both the intent of Individual S to deceive EPA and his/her knowledge of the falsified data in the DMRs. In other words, the jury must be persuaded that the alleged falsifications of the reports were not the result of inadvertent or computer errors. These facts will be proven in most cases through the testimony of witnesses who observed or overheard Individual S planning, setting up or creating the false reports.

Where the false data is contained in the DMRs from the very beginning, details about Company A's computer security system will be irrelevant. Only in cases of actual tampering with the data that Company A intended to send to EPA -- such as where Individual S changed

data after the DMRs were electronically created but before they had been transmitted to EPA -- will evidence about the level of security in Company A's computer system and the resulting difficulty of access possibly persuade the jury that, to accomplish the fraud, Individual S must have known what he or she was doing and intended to deceive.

Thus, in a criminal fraud case, EPA's proof regarding electronic reports must be sufficient to establish (1) the reports' relevance and competence and (2) unequivocally that the individual defendant is the person responsible for transmitting the allegedly fraudulent reports. The remaining elements of most criminal fraud cases will be proven through other evidence that is unrelated to the electronic reporting process and will be no different from cases involving paper reports.

B. False CEM Scenario

Company B submits electronic continuous emissions monitoring (CEM) reports to EPA, some of which, on their face, reflect emissions in excess of the company's air permit. EPA decides to file an action for civil penalties for the permit violations reflected in the CEM reports. For purposes of this discussion, EPA must prove the following elements:

- Company B produced emissions into the ambient air;
- Those emissions contained pollutants reflected in the CEMs that Company B filed electronically with EPA; and
- Those air pollutants exceeded the amounts authorized in Company B's Title V operating permit.

EPA needs to rely on the CEMs to demonstrate that Company B emitted air pollutants in violation of the limitations in its permit. Therefore, EPA wants to have the CEMs introduced into evidence and have the fact-finder accept the data in the CEMs as relevant and competent. Just as in a criminal fraud case, to have the CEMs introduced into evidence, EPA will need to provide witnesses who can testify about the relevance and competence of the CEMs.

All the types of evidence described in the DMR Scenario for acceptance of the DMRs into evidence will be equally necessary in an enforcement action against Company B to recover civil penalties based on the CEMs. They do not include, however, the additional evidence EPA

will have to submit to prove and justify recovery of its proposed civil penalty. In this case, EPA will follow the same process outlined in the DMR Scenario and offer similar testimony of similar witnesses to lay the appropriate foundation for introducing the CEMs into evidence.

After EPA follows the process outlined above to establish that the CEMs are authentic, relevant and not hearsay, the fact-finder will have to determine if the CEMs can be accepted into evidence. If they are, EPA will then call a witness to compare the CEMs to the air pollutant limits in Company B's permit. This witness will allow the fact-finder to determine whether a violation of Company B's air permit limits has occurred, as documented in the electronically filed CEMs.

## V. IMPLICATIONS FOR DEVELOPMENT OF EPA'S APPROACH TO ELECTRONIC REPORTING

Absent clear case law or definitive statutes addressing the evidentiary impact of electronic reports, EPA may need to adopt one or a combination of several options to resolve these problems of proof in criminal and civil enforcement cases. These options include providing additional controls in the process, obtaining additional proof in cases where enforcement is sought, and adopting transaction-specific rules or agreements to ensure the admissibility and reliability of electronic reports. This section briefly identifies some issues for EPA to consider in developing and implementing its electronic reporting policy.

One approach for resolving most of the evidentiary issues outlined in this paper is for EPA to obtain, in advance, an admission from a potential opponent -- the individual who creates the electronic report -- that the report and the data contained in it are genuine and accurate. This commitment could be included in an agreement signed by the individual transmitting the report/data before EPA accepts the electronic transmission, such as through the Terms and Conditions (T&C) Agreement set forth in EPA's 1996 Policy on electronic reporting[3].

The T&C Agreement is intended to create legally binding obligations on those who

---

[3] U.S. Environmental Protection Agency, "General Policy for Accepting Filing of Environmental Reports via Electronic Data Interchange (EDI)," 61 Fed. Reg. 46683-46694 (September 4, 1996).

submit electronic reports to EPA and to
ensure that such reports will be treated as admissible evidence in enforcement cases on the same basis as paper reports. The submitter agrees not to contest the validity or enforceability of electronically signed documents under the FRE and is required to adopt an electronic signature which will serve as evidence that the individual who signs the reports has authority both to send them and to verify the accuracy of their contents. The submitter agrees to sign every report using an electronic identifier and commits that the use of this identifier "constitutes certification of the truth and accuracy, upon penalty of perjury" of the contents of each report. The agreement also provides that a report is "conclusively presumed as a matter of law" to have been signed if the electronic identifier agreed upon by EPA and the submitter is used in accordance with the authentication procedure agreed to by the parties. 61 Fed. Reg. 46689.

A T&C Agreement could help EPA to avoid confronting authenticity questions in particular enforcement or criminal fraud cases against an individual who signs the Agreement. It is not at all clear, however, that a T&C Agreement signed by a corporate entity would have much value in an enforcement case against an individual accused of criminal fraud. Nor does the T&C Agreement resolve other potential evidentiary questions that may be raised by the defense in a criminal case in order to create a reasonable doubt in the jurys' minds. Such defenses might include allegations of either inadvertent or intentional alteration of the data during transmission to EPA or during storage and retrieval by the agency.

Moreover, there are not yet any court decisions testing the use and evidentiary effects of a T&C Agreement. EPA's agreement arguably goes beyond resolving the traditional evidentiary issues of the authenticity and accuracy of submitted data. It also asks the submitter to stipulate to the truthfulness and accuracy of the contents of each report, and thereby formally forecloses the individual or corporate entity signing the agreement from a later collateral challenge to the veracity of the information in the report. In a criminal case, courts may not be receptive to relying on such an admission thereby depriving a defendant of the ability to impeach the data in an electronic report when it is introduced into evidence by the prosecution.

If a T&C Agreement regarding the admissibility of electronic reports is accepted, however, the remaining implications discussed in this section would come into play only in cases where the submitter later claims that the written version of the report offered into evidence differs from the data that was electronically filed. Based on EPA's proposed policy and process for electronic reporting, the government should be prepared to submit proof in the following three areas to authenticate all electronic reports:

- o Genuineness of the message contents;
- o Reliability of the message record as sent and received; and
- o Chain of custody.

In any particular case, prosecutors will need to gather evidence to establish the genuineness of the data contained in the electronic report. They will also need evidence to document the reliability of the entire electronic transmission process from data entry by an individual working for the regulated entity through data retrieval by EPA staff, both for normal agency purposes and, ultimately, for submission to the fact-finder in an enforcement case. Proof of the security and reliability of the transmission and storage component of EPA's electronic reporting process -- the "black box" aspect -- is also a necessary and very important part of authenticating electronic reports.

For electronic reports to qualify as business records that will be admissible as an exception to the hearsay rule, all aspects of the reporting process -- data creation, entry, storage, transmission, receipt and retrieval -- must be "regular." In other words, the process must be the same for all users of the electronic reporting and data transfer system. The regularity of the process will also be an essential element of a case in which EPA wishes to prove that a required report was <u>not</u> ever filed.

The fact-finder's perception of the regularity and reliability of the electronic reporting process will be increased in direct proportion to the simplicity of the process. As a result, the fewer the opportunities allowed by the process for the data to be changed -- whether intentionally or unintentionally -- from data creation through retrieval, the more likely that a jury will be able to understand and be persuaded by the evidence about electronic reports. Viewed a different way, every additional step in the process means another link in the chain of custody which offers an opportunity for the defense to create doubts in the mind of the fact-finder or the jury about the strength or reliability of the electronic reporting process.

To create doubt in the minds of lay people who do not have complete knowledge of the mechanics of electronic data transfer and storage, a defendant can argue that the reliability of an electronic report is potentially compromised each time it is transferred, archived, or otherwise manipulated. EPA will need to prove that electronic reports retrieved from EPA's computers and presented to the fact-finder in printed form contain the same data which an individual working for the regulated entity entered into its computer and sent to EPA. Thus, evidence about each

instance of data creation, entry, transfer, archiving, storage or other manipulation may be necessary to establish the reports' genuineness and chain of custody. Such evidence will be necessary to overcome any reasonable doubt in the jurys' minds so the government can sustain its burden of proof.

Security features for an electronic reporting process must serve at least two purposes:

- o They must support verification of the identity of the electronic submitter; and
- o They must allow detection of any errors or manipulation of the data.

To establish liability of an individual in any case related to electronic reports, the identity of the person who submitted the data must be proven. In all criminal fraud cases and in other criminal enforcement cases seeking to hold an individual liable, the identity of the submitter must be proven beyond a reasonable doubt. The security features incorporated in EPA's policy on electronic reporting must therefore enable the government to establish the submitter's identity -- probably by an electronic "signature" -- to satisfy this high level of proof. Proof of security features that reduce the possibility of data alteration will likely be required in every EPA enforcement case, at least until case law catches up with technology and judicial presumptions are established or until judicial notice is regularly taken of electronic reporting and data transfers.

There has been very little legal analysis so far of the problems presented when electronic data are used as evidence in enforcement actions. There is, however, a developing body of analysis examining the potential role of electronic data transfers in the area of commercial transactions. One expert on this subject has outlined an approach to creating an enforceable data transfer system which may have significant instructive value for a government reporting system.[4] He advocates incorporating the following four features when designing any electronic data transfer system which may ultimately be tested in the crucible of litigation:

- o Controls over original data input, which ensure that transaction originators are identified and message contents are accurate and complete;

---

[4] Benjamin Wright. *The Law of Electronic Commerce: EDI, E-mail and Internet: Technology, Proof, and Liability*. Second Edition, 1996.

- o Controls over transmission of data to preserve message contents and provide proper delivery and processing;

- o Controls over record creation, indexing and storage; and

- o Security features throughout the system to preclude intentional tampering with messages and records.

These principles can be directly applied to EPA's electronic reporting system and to the evidentiary issues which EPA may face in seeking admission of electronic reports as evidence in an enforcement proceeding. First, EPA must focus on developing methods to identify conclusively the "individual transaction originator" in order to be able to authenticate challenged electronic reports as emanating from the individual who is the defendant in an enforcement action and to convince a fact-finder to admit the reports into evidence.

Second, EPA must develop effective but reasonably transparent controls over the transmission, receipt, storage and retrieval of electronic data. Those controls must be sufficiently strong to overcome defendants' evidentiary challenges to any electronic reports relied upon by EPA. EPA can expect defendants to challenge the reliability, relevance and chain of custody of all electronic data which EPA needs to prove its case.

Ultimately, EPA must design a system which incorporates sufficient safeguards to preclude -- in a manner which the government can demonstrate at trial -- either inadvertent or intentional alteration of the original report and the data it contained. In short, the four features listed above can serve as a useful shorthand or proxy for measures which will enable EPA to meet its evidentiary needs and burden of proof for successful prosecution of enforcement cases, including criminal fraud cases, that involve electronic reports.

## V. CONCLUSION

This memorandum has provided an overview of the applicable federal evidentiary rules and an outline of the proof needed for EPA to prosecute successfully enforcement actions that rely on electronic reports. In addition, the memorandum has briefly examined some of the issues that EPA should consider in developing its policy on electronic reporting. In light of the rapidly evolving technologies and newly developing case law for electronic reporting, more research and analysis will be needed as EPA further develops and implements its electronic reporting policy.